ELECTRONIC CIRCUIT FOR RANDOM NUMBER GENERATION

--This application claims priority to Serial Number 60/454,814 filed March 14, 2003.--

FIELD OF THE INVENTION

[0001] The invention relates to the phenomenon of metastability and the effect of metastability on semiconductors. More particularly, the present invention relates to an increase in the randomness of a random number generator, and its ability to withstand environmental changes better than known in the prior art.

BACKGROUND ART

[0002] Latches and flip-flops are widely used in all types of electronic devices for counting, sampling, and storage of data. There are a number of different types of flip-flops named after their primary function, such as D-type flip-flops (data), J-K flip flops (J and K inputs), and R-S flip-flops (having R and S latches, standing for "reset: and "set". D flip-flops are a clocked flip-flop having a one clock pulse delay for its output.

[0003] However, the operating conditions of the flip-flops can be violated because hold times and setup times are not always consistent with the specifications (such as provided in the data sheets) of the flip flops used. The violation of the operating conditions of the flip-flops can cause them to go into an unstable (metastable) state that can affect the entire operation of the linked systems. Metastability can occur when both inputs to a latch are set at a logic high (11) and are subsequently set at a logic low (00).

[0004] Metastability can cause the latch outputs to oscillate unpredictably in a statistically known manner. Such metastable values are then detected by other circuitry as different logic states. It has been realized by both the present inventor and others in the art that the unpredictability of the oscillations could be useful as a random number generator for a multitude of practical uses.

[0005] Current designs of physical (true) random number generators based on flip-flop metastability used fixed delay values between their inputs to violate setup and hold timings, in order to provoke metastability. Eventually, the metastable state resolves to some logic level, which is effectively random, depending on the internal noise of the flip-flops.

However, the fixed delay values used by the prior art can cause the random number generator to be susceptible to environmental changes. In addition, fixed delay values at large manufacturing variations can make the circuit not work at all or not work at optimal speed.

SUMMARY OF THE INVENTION

[0006] The present invention provides a physical random number generator using only standard digital components. The circuit stops and starts two free running oscillators. The instantaneous voltage of the oscillators at the time of stop do not usually reach true logic levels (i.e. cannot be discerned as a 0 or 1). These voltage levels are applied to the inputs of a bi-stable digital device (latch, flip-flop) provoking metastability. The metastable state eventually resolves in settling to a final standard logic state. The logic value to which the circuit settles depends on the instantaneous voltage (affected by the phase drifts) of the two free running oscillators and the resolution of the metastable states. Thus, the final value of the random number generator circuit of the instant invention is more random than previous prior art circuits, as well as being more tolerant to environmental changes than such prior art circuitry.

BRIEF DESCRIPTION OF THE DRAWING

[0007] Fig. 1A illustrates one arrangement of a random number generator according to the present invention. As the switches are shown the inverters are not connected to each other, oscillator feedback loops are closed so the inverters form two independent free running oscillators.

[0008] Fig. 1B illustrates the random number generator shown in Fig. 1A having the oscillator feedback loops opened and the inverters cross-connected. As the switches are shown the cross-connected inverters form a latch.

[0009] Figs. 2A-2C illustrate some of the many variations of the present invention.

DETAILED EMBODIMENTS

[0010] Figs. 1A and 1B illustrate one arrangement of a random number generator according to the instant invention. It is understood by persons of ordinary skill in the art that the type of gates shown was selected for explanatory purposes, and there can be different arrangements of different type of gates (NAND, NOR, XOR, etc.) in terms of size, function and connectivity that fall within the spirit of the invention and the scope of the appended claims.

[0011] With regard to Fig. 1A, a clock 105 provides an input to D flip-flop 110. The Q (non-inverted) output of the D flip-flop is connected to switches 115,120, and the inverted Q output is fed back to the D input so that the flip-flop provides a square wave output on both the normal and inverted D and D bar. The switches 115,120 can be referred to as oscillator feedback switches. If the two switches 115,120 are closed and the switches 118, 119 are open as shown in the diagram above, the two inverters 117,122 form two independent free running (ring) oscillators. A latching device 125 connected to at least one of the oscillator outputs will permit a reading of a random generated bit when the cross gate switches 118,119 are reopened.

[0012] The delay elements 116, 123 can be implemented, for example, as a series of buffer gates or an even number of inverters (0, 2, 4...). The corresponding delay values should be sufficiently different (e.g. 5 and 7 buffers) such that in case of a strong external signal there is little chance that both oscillators would synchronize to it. The delay devices can be different lengths of wires.

[0013] As shown in Fig. 1B, the inverters 117, 122 of the random number generator form a latch by having their gates cross-connected via the closing of switches 118, 119 (and opening the switches 115, 120). Due to positive feedback, the cross connected gates eventually latch up, resolving to a logic state. In order to read a random-generated bit, the output of one of the inverters can be latched at the time of opening the switches 119,118 to latch mechanism 125.

[0014] As shown in Fig. 1B, the random number generator shown of in Fig. 1A has the oscillator feedback loops opened (by the opening of switches 115, 120) and the inverters

cross-connected by the closing of switches 118, 119. By opening the feedback loops, the free running oscillators are stopped. The relative and absolute values of the instantaneous output voltages and the internal noise determine the logic state to which the newly formed latch circuit will settle in. Thus, the two free-running oscillators are effectively sampled at the pace of an independent clock 115 and occasional metastable states of the sampling latch resolve to a random final logic state. The pair of oscillators (inverters) forms a bi-stable device with positive feedback resolving to a logic state by opening the feedback loop switches and closing the cross gate switches.

[0015] Metastability can come in the following ways:

[0016] 1. When the oscillators are switched on there is a delay from the switching on to their starting. This delay (or hesitation) causes the voltage to go up or down for a short period of time, thereby creating an uncertain starting point. It should be noted that in a best mode the loop gain must be small; otherwise the oscillators may start immediately without the delay (a.k.a. hesitation).

[0017] 2. When the oscillators are stopped, the gates become cross-connected. At this point one or both output voltages could be between logic levels. The flip-flop, which is formed by the two inverters, has to settle to a logic state. However, the settling to a logic state occurs in a metastable way, the oscillation does not stop immediately, with the period becoming gradually longer and longer until the voltages resolve to their final value.

[0018] It should be noted that the instant invention uses CMOS logic gates not in digital but in analog mode. In addition, it should be understood that there are various modifications that may be made by a person of ordinary skill in the art that do not depart from the spirit of the invention and the scope of the appended claims. For example, the last delay gate could be of a tri-state type, when switching the loop requires activating/deactivating the high impedance output. The number of inverters can be different, as could the number or type of switches used.

[0019] Figs. 2A-2C illustrate some variations of how the instant invention can be practiced. For example, with regard to Fig. 2A, the last delay gate could be of a tri-state type, and switching the loop requires activating the high impedance output.

[0020] With regard to Fig. 2B, a straightforward implementation uses transition gates 228-231, which are essentially analog switches. Although it is true that most standard CMOS logic component libraries no longer include the transition gates, this configuration is still possible for those that do include such gates.

[0021] Fig. 2C illustrates one of the easiest ways to implement the randomness source through the use of two inverting multiplexers 232,233. When their S_1 inputs are activated, they both form ring oscillators. When their S_2 inputs get activated, two cross connected inverters result, forming a latch. A latch mechanism 125 is connected to one of the outputs of the multiplexers.

[0022] It will be appreciated by an artisan that the claimed invention has significant breadth and should not be limited to the aspects shown and described. For example, the pair of oscillators with at least one delay device may constitute a simple version of the invention.

[0023] Also, it is to be understood by persons of ordinary skill in the art that a "delay device" may comprise a length of wire, with different delays afforded different lengths of wire.

[0024] While the use of switches for cross gate and feedback loops is preferred, they are not required and could also vary in number other than four. While it is preferable that the switches be controlled by a flip-flop, such a device is not a requirement to practice the claimed invention. In addition, the type of flip-flop, or another type of driver could be used, if driving the oscillators or switches of the inverters are desired. An artisan appreciates these differences as lying within the spirit of the invention and the scope of the appended claims.